The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
02/14/2017

SUBJECT:
Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution (APSB17-04)

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Flash Player, the most severe of which could allow for remote code execution. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation of the most severe of these vulnerabilities could result in the attacker gaining control of the affected system.

THREAT INTELLIGENCE:
There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Adobe Flash Player Desktop Runtime versions 24.0.0.194 and earlier
- Adobe Flash Player for Google Chrome versions 24.0.0.194 and earlier
- Adobe Flash Player for Microsoft Edge and Internet Explorer 11 versions 24.0.0.194 and earlier

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Adobe Flash Player is prone to multiple vulnerabilities, the most severe of which could allow for remote code execution.

- A type confusion vulnerability that could lead to code execution (CVE-2017-2995).
- An integer overflow vulnerability that could lead to code execution (CVE-2017-2987).
- Multiple use-after-free vulnerabilities that could lead to code execution (CVE-2017-2982, CVE-2017-2985, CVE-2017-2993, CVE-2017-2994).

- Multiple heap buffer overflow vulnerabilities that could lead to code execution (CVE-2017-2984, CVE-2017-2986, CVE-2017-2992).
- Multiple memory corruption vulnerabilities that could lead to code execution (CVE-2017-2988, CVE-2017-2990, CVE-2017-2991, CVE-2017-2996).

Successful exploitation of the most severe of these vulnerabilities could result in the attacker gaining control of the affected system.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Adobe:

https://helpx.adobe.com/security/products/flash-player/apsb17-04.html

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2982
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2984
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2985
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2986
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2987
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2988
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2990
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2991
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2992
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2993
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2994
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2995
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2996